Non Abelian Bent Functions

Laurent Poinsot

Noname manuscript No.
(will be inserted by the editor)

Non Abelian Bent Functions

Laurent Poinsot

the date of receipt and acceptance should be inserted later

Abstract Perfect nonlinear functions from a finite group G to another one H are those functions $f : G \to H$ such that for all nonzero $\alpha \in G$, the derivative $d_\alpha f : x \mapsto f(\alpha x)f(x)^{-1}$ is balanced. In the case where both G and H are Abelian groups, $f : G \to H$ is perfect nonlinear if and only if f is bent *i.e.* for all nonprincipal character χ of H, the (discrete) Fourier transform of $\chi \circ f$ has a constant magnitude equals to $|G|$. In this paper, using the theory of linear representations, we exhibit similar bentness-like characterizations in the cases where G and/or H are (finite) non Abelian groups. Thus we extend the concept of bent functions to the framework of non Abelian groups.

Keywords Bent functions · perfect nonlinearity · finite non Abelian groups · Fourier transform.

Mathematics Subject Classification (2000) 11T71 · 20B05 · 43A30

1 Introduction

Let G and H be two finite groups (in multiplicative representation). Perfect nonlinear functions from G to H are those ideal functions $f : G \to H$ that match the less possible with the pattern of group homomorphism *i.e.* such that for all nonzero $\alpha \in G$ and for all $\beta \in H$,

$$|\{x \in G | f(\alpha x)f(x)^{-1} = \beta\}| = \frac{|G|}{|H|}. \tag{1}$$

When G and H are both (finite-dimensional) vector spaces over $\mathrm{Z}_2 = \{0, 1\}$, these functions, originally introduced by Nyberg [5], exhibit the maximal resistance against the differential attack [1]. Also in the Boolean case, this notion is

LIPN-UMR CNRS 7030, Institut Galilée, Université Paris-Nord 99, avenue Jean-Baptiste Clément 93430 Villetaneuse, France,
E-mail: laurent.poinsot@lipn.univ-paris13.fr

known to be equivalent to bent functions: $f : \mathrm{Z}_2^m \to \mathrm{Z}_2^n$ is bent if for all $\alpha \in \mathrm{Z}_2^m$ and for all nonzero β in Z_2^n,

$$|\widehat{(\chi^{\beta}_{\mathbb{Z}_2^n} \circ f)}(\alpha)|^2 = 2^m \tag{2}$$

where $\chi^{\beta}_{\mathbb{Z}_2^n} : \mathrm{Z}_2^n \to \{\pm 1\}$ is defined at y by $(-1)^{\beta.y}$ (the point in exponent is the natural dot-product of Z_2^n) and

$$\widehat{\phi}(\alpha) = \sum_{x \in \mathbb{Z}_2^m} \phi(x)(-1)^{\alpha.x} \tag{3}$$

is the Fourier transform of $\phi : G \to \mathrm{C}$ (this time $\alpha.x$ is the dot-product in Z_2^m). These functions, independently introduced by Dillon [3] and Rothaus [9], exhibit the maximal resistance against the linear attack [4].
The equivalence between bentness and perfect nonlinearity has been recently extended by Carlet and Ding [2] and Pott [8] to the general case: $f : G \to H$ (where G and H are two finite Abelian groups) is perfect nonlinear if and only if for all $\alpha \in G$ and for all nonprincipal character χ of H,

$$|\widehat{(\chi \circ f)}(\alpha)|^2 = |G| \tag{4}$$

where for $\phi : G \to \mathrm{C}$, $\widehat{\phi}$ is its discrete Fourier transform.
In this paper, we exhibit the same kind of characterizations in the case where at least one of the two finite groups G and H is non Abelian. This gives a general equivalence between perfect nonlinearity and bentess.

Outline of the paper

Next section contains the general notations used in the paper. In sect. 3 are recalled some of the main results on the duality of finite groups. In particular, we present several kind of Fourier transforms used in the new characterizations of perfect nonlinearity in the non Abelian cases. The notion of perfect nonlinearity is exposed in the general framework of finite groups in sect. 4. Also in this section is given the dual characterization - *i.e.* the notion of bentness - of Carlet, Ding [2] and Pott [8] of perfect nonlinear functions in the Abelian groups setting. Finally our own results of non Abelian bentness are developed in sect. 5.

2 Notations

$|S|$ is the cardinality of any finite set S and if S is nonempty (possibly infinite), Id_S denotes its identity map.
In this paper, the capital letters "G" and "H" always denote finite groups in multiplicative representation, e_G is the neutral element and G^* is defined as $G \setminus \{e_G\}$.
The vector spaces considered are always finite-dimensional complex vector spaces. For a (complex) vector space V, 0_V is its zero, $\dim_{\mathbb{C}}(V)$ is its dimension and $GL(V)$ denotes the *linear group* of V which is a subset of the vector space of all endomorphisms of V, denoted $End(V)$. If λ is any linear map, λ^* denotes its adjoint and

the *unitary group* of V is $\mathrm{U}(V)$.

By convention, for each known result recalled in this paper, the proof has been intentionally omitted and a reference - not necessarily *the* original reference - is given. On the contrary, our own results are given obviously with their proofs and without any reference.

3 On the duality of finite groups

3.1 Introduction

This paper is dedicated to the establishment of a dual characterization of the concept of perfect nonlinearity - similar to the one given by Carlet and Ding [2] and Pott [8] concerning Abelian groups - in the non Abelian groups setting, using some harmonic analysis techniques. So in this section, we recall some basics about the duality of finite groups and the Fourier transform. Most of the definitions and results given in this section are well-known and can be found in any book on finite groups ([6] for instance).

3.2 The Abelian case

3.2.1 The theory of characters

Definition 1 Let G be a finite group. A *character* χ of G is a group homomorphism from G to the multiplicative group C^*. We denote by $\widehat{G}$ the set of all characters, called *dual* of G.

The set $\widehat{G}$ is actually a group under the point-wise multiplication of characters and its elements are valued in the group of the $|G|^{th}$ complex roots of the unity. In particular,

$$\forall \chi \in \widehat{G},\ \forall x \in G,\ |\chi(x)| = 1 \text{ and } \chi(x^{-1}) = \overline{\chi(x)} \tag{5}$$

where $|z|$ is the complex-modulus and $\overline{z}$ is the conjugate of $z \in \mathrm{C}$.

Proposition 1 *([6]) Let G be a finite Abelian group. Then G and $\widehat{G}$ are isomorphic.*

In the remainder of this paper, when a finite Abelian group G is considered, we always implicitly suppose that an isomorphism from G to G^* has been fixed and we use χ_G^α to denote the image of α by such an isomorphism. In particular, $\forall x \in G$, $\chi_G^{e_G}(x) = 1$ (this character is called *trivial* or *principal*). Finally the characters satisfy the well-known orthogonality properties.

Lemma 1 *([6]) Let G be a finite Abelian group. For all $\alpha \in G$ we have*

$$\sum_{x \in G} \chi_G^\alpha(x) = \begin{cases} 0 & \text{if } \alpha \in G^*, \\ |G| & \text{if } \alpha = e_G. \end{cases} \tag{6}$$

For all $x \in G$, we have

$$\sum_{\alpha \in G} \chi_G^\alpha(x) = \begin{cases} 0 & \text{if } x \in G^*, \\ |G| & \text{if } x = e_G. \end{cases} \tag{7}$$

3.2.2 The (discrete) Fourier transform

Definition 2 Let G be a finite Abelian group. The *Fourier transform* of $\phi : G \to \mathbb{C}$ is the map $\widehat{\phi} : G \to \mathbb{C}$ defined for $\alpha \in G$ by

$$\widehat{\phi}(\alpha) = \sum_{x \in G} \phi(x) \chi_G^\alpha(x). \tag{8}$$

Some well-known and useful results are summarized below for G a finite Abelian group.

Proposition 2 *([6]) Let $\phi : G \to \mathbb{C}$.*

1. *We have the inversion formula*

$$\phi = \frac{1}{|G|} \sum_{\alpha \in G} \widehat{\phi}(\alpha) \overline{\chi_G^\alpha}; \tag{9}$$

2. *We have the Parseval's equation*

$$\sum_{x \in G} |\phi(x)|^2 = \frac{1}{|G|} \sum_{\alpha \in G} |\widehat{\phi}(\alpha)|^2; \tag{10}$$

3. *$\phi(x) = 0 \ \forall x \in G^*$ if and only if $\widehat{\phi}$ is constant;*
4. *$\widehat{\phi}(\alpha) = 0 \ \forall \alpha \in G^*$ if and only if ϕ is constant.*

Concerning the last two points, their proofs can be checked in [2].

3.2.3 The multidimensional (discrete) Fourier transform

In subsection B. of sect. 5, we consider some V-valued functions, where V is a finite-dimensional vector space, defined on a finite Abelian group G and we need to compute their "Fourier transforms". That is the reason why we now introduce a natural extension of the discrete Fourier transform, called *multidimensional Fourier transform*, to deal with V-valued functions rather than $\mathbb{C}$-valued ones. More details on this transform should be found in [7].

Definition 3 Let G be a finite Abelian group, V a finite-dimensional vector space over $\mathbb{C}$ and $\phi : G \to \mathbb{C}$. The *multidimensional Fourier transform* of ϕ is defined as

$$\begin{aligned} \widehat{\phi}^{MD} : G &\to V \\ \alpha &\mapsto \sum_{x \in G} \chi_G^\alpha(x) \phi(x). \end{aligned} \tag{11}$$

Now let suppose that V is equipped with an inner-product (linear in the first variable and anti-linear in the second) denoted $\langle ., . \rangle_V$. Let fix B an orthonormal basis of V. For each $e \in B$, we define the *component function* ϕ_e of $\phi : G \to V$ in direction e as the map

$$\begin{aligned} \phi_e : G &\to \mathbb{C} \\ x &\mapsto \langle \phi(x), e \rangle_V. \end{aligned} \tag{12}$$

According to the properties of orthonormal basis, we have $\forall x \in G$,

$$\phi(x) = \sum_{e \in B} \phi_e(x) e. \tag{13}$$

We can easily check that the multidimensional Fourier transform is actually a component-wise discrete Fourier transform given by the following equation (for $\alpha \in G$)

$$\widehat{\phi}^{MD}(\alpha) = \sum_{e \in B} \widehat{\phi_e}(\alpha) e. \tag{14}$$

Using this last equation, we can establish an *inversion formula* for the multidimensional Fourier transform. Let $x \in X$.

$$\begin{aligned}
\phi(x) &= \sum_{e \in B} \phi_e(x) e \\
&= \sum_{e \in E} \left(\frac{1}{|G|} \sum_{\alpha \in G} \widehat{\phi_e}(\alpha) \overline{\chi_G^\alpha}(x) \right) e \\
&\quad \text{(by the inversion formula applied on } \phi_e) \\
&= \frac{1}{|G|} \sum_{\alpha \in G} \overline{\chi_G^\alpha(x)} \left(\sum_{e \in B} \widehat{\phi_e}(\alpha) e \right) \\
&= \frac{1}{|G|} \sum_{\alpha \in G} \overline{\chi_G^\alpha(x)} \widehat{\phi}^{MD}(\alpha).
\end{aligned} \tag{15}$$

Finally this transform satisfies a result similar to the third point of proposition 2.

Proposition 3 *Let G be a finite Abelian group, V a finite-dimensional vector space over $\mathbb{C}$ and $\phi : G \to V$. We have $\phi(x) = 0_V$ for all $x \in G^*$ if and only if $\widehat{\phi}^{MD}(\alpha) = \phi(e_G)$ for all $\alpha \in G$.*

Proof $\Rightarrow$) Let suppose that for all $x \in G^*$, $\phi(x) = 0_V$. Then we have $\forall \alpha \in G$, $\widehat{\phi}^{MD}(\alpha) = \sum_{x \in G} \chi_G^\alpha(x) \phi(x) = \phi(e_G)$.

$\Leftarrow$) Let suppose that $\widehat{\phi}^{MD}(\alpha) = \phi(e_G)$ for all $\alpha \in G$. Using the inversion formula (15), we get that for $x \in G$, $\phi(x) = \frac{1}{|G|} \left(\sum_{\alpha \in G} \overline{\chi_G^\alpha(x)} \right) \phi(e_G) = \begin{cases} 0_V & \text{if } x \in G^*, \\ \phi(e_G) & \text{if } x = e_G, \end{cases}$ according to the orthogonality relations (lemma 1).

□

3.3 The non Abelian case

3.3.1 The theory of linear representations

Definition 4 Let V be a finite-dimensional complex vector space. A *linear representation* of a finite group G on V is a group homomorphism from G to $GL(V)$.

For each linear representation $\rho : G \to GL(V)$, it is possible to find a basis of V in which for all $x \in G$, $\rho(x)$ is a unitary operator of V *i.e.* $\rho : G \to \mathrm{U}(V)$. Indeed, we can check that for a linear representation ρ of G on V, for each $x \in G$, $\rho(x)$ leaves invariant the following inner-product in V

$$\langle u, v\rangle_{G,\rho,V} = \sum_{x\in G} \langle \rho(x)(u), \rho(x)(v)\rangle_V \tag{16}$$

where $(u, v) \in V^2$ and $\langle ., .\rangle_V$ denotes any inner-product of V (linear in the first variable and anti-linear in the second). Then in the remainder, without loss of generality, we only consider unitary representations.

The linear representations of G on C can be identified with the characters of G since C and $GL(\mathrm{C})$ are isomorphic. Actually if G is a finite Abelian group then the notion of linear representation gives nothing new because it is equivalent to the notion of character.

Definition 5 A linear representation ρ of a finite group G on V is said to be *irreducible* if there is no subspace $W \subset V$, other than $\{0_V\}$ and V, such that $\forall x \in G$, $\forall w \in W$, $\rho(x)(w) \in W$.

Definition 6 Two linear representations ρ and ρ' of a finite group G on respectively V and V' are *isomorphic* if it exists a linear isomorphism $\Phi : V \to V'$ such that for all $x \in G$,

$$\Phi \circ \rho(x) = \rho'(x) \circ \Phi. \tag{17}$$

(A linear map that satisfies equality (17) is called *equivariant map* and is easily seen to be a morphism from V to V' seen as left G-modules.)

The notion of isomorphism is an equivalence relation for linear representations[1].

Definition 7 For a finite group G, the *dual* of G, denoted $\widetilde{G}$, is a set that contains exactly one and only one representative of each equivalence class of isomorphic irreducible representations of G.

By definition, if $(\rho, \rho') \in \widetilde{G}^2$, then ρ and ρ' are nonisomorphic irreducible representations of G. In the remainder, the notation

$$\rho = \rho_V \in \widetilde{G} \tag{18}$$

means that $\rho : G \to \mathrm{U}(V)$ is an irreducible representation of G.
If G is a finite Abelian group, then $\widetilde{G}$ is equal to $\widehat{G}$ (up to an isomorphism from $GL(\mathrm{C})$ to C). If G is a finite non Abelian group, the two notions of duality become distinct (in particular, $\widetilde{G}$ is not a group). By abuse of notation, $\widetilde{G}^*$ is defined as the set $\widetilde{G} \setminus \{\rho_0\}$ where ρ_0 is the *trivial* or *principal* representation of G *i.e.* $\forall x \in G$, $\rho_0(x) = Id_{\mathbb{C}}$.

When dealing with linear representations, a major result, know as *Schur's lemma*, should be kept in mind.

[1] Even if the collection of all linear representations of a given finite group does not form a set but rather a proper class, it is an easy exercice to check that the collection of isomorphism classes of linear representations really does form a set.

Lemma 2 *([6]) Let G be a finite group. Let $\rho = \rho_V \in \widetilde{G}$ and $\lambda \in End(V)$. If $\forall x \in G$, $\lambda \circ \rho(x) = \rho(x) \circ \lambda$ then λ is a multiple of the identity i.e. it exists $k \in \mathbb{C}$ such that $\lambda = kId_V$.*

As direct consequences of the Schur's lemma, we can state the two following results that will be use in the sequel.

Lemma 3 *([6]) Let G be a finite group. For $x \in G^*$,*

$$\sum_{\rho_V \in \widetilde{G}} \dim_{\mathbb{C}}(V) tr(\rho_V(x)) = 0 \tag{19}$$

where "tr" denotes the usual trace of endomorphisms.

Lemma 4 *Let G be a finite group. Let $\rho = \rho_V \in \widetilde{G}^*$. Then*

$$\sum_{x \in G} \rho(x) = 0_{End(V)}. \tag{20}$$

Proof Let $\lambda \in End(V)$ defined as $\lambda = \sum_{x \in G} \rho(x)$. Let $x_0 \in G$. We have

$$\lambda = \sum_{x \in G} \rho(x) = \sum_{x \in G} \rho(x_0 x) = \rho(x_0) \circ \sum_{x \in G} \rho(x) = \rho(x_0) \circ \lambda$$

but also

$$\lambda = \sum_{x \in G} \rho(x) = \sum_{x \in G} \rho(x x_0) = \left(\sum_{x \in G} \rho(x) \right) \circ \rho(x_0) = \lambda \circ \rho(x_0).$$

In particular $\lambda \circ \rho(x_0) = \rho(x_0) \circ \lambda$. As it is true for any $x_0 \in G$, λ commutes with all $\rho(x)$. By the Schur's lemma, λ is a multiple on the identity: it exists $k \in \mathbb{C}$ such that $\lambda = kId_V$. Now let suppose $\lambda \neq 0_{End(V)}$, then $k \in \mathbb{C}^*$. Using the first part of the proof, we know that $\lambda = \rho(x) \circ \lambda$ (for each $x \in G$). Then $(Id_V - \rho(x)) \circ \lambda = 0_{End(V)}$. As $\lambda = kId_V$, we have $(Id_V - \rho(x)) \circ (kId_V) = 0_{End(V)}$. Since $k \neq 0$, we have $Id_V - \rho(x) = 0_{End(V)}$ or also $\rho(x) = Id_V$ which is a contradiction with the assumption that ρ is non trivial. □

3.3.2 The representation-based Fourier transform

By substituting irreducible linear representations to characters, it is possible to define a kind of Fourier transform for non Abelian groups.
Let G be any finite group.

Definition 8 Let $\phi : G \to \mathbb{C}$. The *(representation-based) Fourier transform* of ϕ is defined for $\rho = \rho_V \in \widetilde{G}$ as

$$\widetilde{\phi}(\rho) = \sum_{x \in G} \phi(x) \rho(x) \in End(V). \tag{21}$$

This notion is a generalization of the classical discrete Fourier transform. This transform is invertible so we have also an *inversion formula*.

Proposition 4 *([6]) Let $\phi : G \to \mathrm{C}$. Then for all $x \in G$ we have,*

$$\phi(x) = \frac{1}{|G|} \sum_{\rho_V \in \widetilde{G}} \dim_{\mathbb{C}}(V) tr(\rho_V(x^{-1}) \circ \widetilde{\phi}(\rho_V)). \tag{22}$$

A last technical lemma is given below.

Lemma 5 *Let $\phi : G \to \mathrm{C}$. We have*

1. *$\phi(x) = 0 \ \forall x \in G^*$ if and only if $\forall \rho = \rho_V \in \widetilde{G}$, $\widetilde{\phi}(\rho) = \phi(e_G) Id_V$;*
2. *$\widetilde{\phi}(\rho) = 0_{End(V)} \ \forall \rho = \rho_V \in \widetilde{G}^*$ if and only if ϕ is constant.*

Proof $1. \Rightarrow)$ For $\rho = \rho_V \in \widetilde{G}$, we have

$$\begin{aligned} \widetilde{\phi}(\rho) &= \sum_{x \in G} \phi(x)\rho(x) \text{ (by definition)} \\ &= \phi(e_G)\rho(e_G) \text{ (by assumption on } \phi) \\ &= \phi(e_G) Id_V \\ &\quad \text{(since } \rho \text{ is a group homomorphism).} \end{aligned}$$

$\Leftarrow)$ For $x \in G$, the inversion formula gives

$$\begin{aligned} &\phi(x) = \frac{1}{|G|} \sum_{\rho_V \in \widetilde{G}} \dim_{\mathbb{C}}(V) tr(\rho_V(x^{-1}) \circ \widetilde{\phi}(\rho_V)) \\ &= \frac{1}{|G|} \sum_{\rho_V \in \widetilde{G}} \dim_{\mathbb{C}}(V) tr(\rho_V(x^{-1}) \circ \phi(e_G) Id_V) \\ &\text{(by hypothesis)} \\ &= \frac{\phi(e_G)}{|G|} \sum_{\rho_V \in \widetilde{G}} \dim_{\mathbb{C}}(V) tr(\rho_V(x^{-1})) \\ &= \frac{\phi(e_G)}{|G|} \sum_{\rho_V \in \widetilde{G}} \dim_{\mathbb{C}}(V) tr(\rho_V(x)^{-1}) \\ &\text{(since } \rho_V \text{ is a group homomorphism)} \\ &= \frac{\phi(e_G)}{|G|} \sum_{\rho_V \in \widetilde{G}} \dim_{\mathbb{C}}(V) tr(\rho_V(x)^*) \\ &\text{(since } \rho_V(x) \text{ is unitary)} \\ &= \frac{\phi(e_G)}{|G|} \sum_{\rho_V \in \widetilde{G}} \dim_{\mathbb{C}}(V) \overline{tr(\rho_V(x))} \\ &= \frac{\phi(e_G)}{|G|} \overline{\sum_{\rho_V \in \widetilde{G}} \dim_{\mathbb{C}}(V) tr(\rho_V(x))} \\ &= 0 \text{ if } x \neq e_G \text{ (according to lemma 3).} \end{aligned}$$

$2. \Rightarrow)$ By the inversion formula, $\forall x \in G$,

$$\begin{aligned} &\phi(x) = \frac{1}{|G|} \sum_{\rho_V \in \widetilde{G}} \dim_{\mathbb{C}}(V) tr(\rho_V(x^{-1}) \circ \widetilde{\phi}(\rho_V)) \\ &= \frac{1}{|G|} tr(\widetilde{\phi}(Id_{\mathbb{C}})) \text{ (by hypothesis).} \end{aligned} \tag{23}$$

$\Leftarrow$) Let $\rho_V \in \widetilde{G}$, we have $\widetilde{\phi}(\rho_V) = k \sum_{x \in G} \rho_V(x)$ (with $\phi(x) = k \ \forall x \in G$). According to lemma 4, we deduce that $\widetilde{\phi}(\rho_V) = 0_{End(V)}$ for all $\rho_V \in \widetilde{G}^*$.

□

4 On perfect nonlinear functions

4.1 Some basic definitions

Perfect nonlinearity must be seen as the fundamental notion on which our results are based. Actually our ambition in this paper is to describe this combinatorial concept in terms of Fourier transforms. Thus it is necessary to briefly present this topic.

Definition 9 Let X and Y be two finite nonempty sets. A function $f : X \to Y$ is said to be *balanced* if the function

$$\begin{aligned} \phi_f : Y &\to \mathrm{N} \\ y &\mapsto |\{x \in X | f(x) = y\}| \end{aligned} \tag{24}$$

is constant equal to $\dfrac{|X|}{|Y|}$.

Definition 10 Let G and H be two finite groups and $f : G \to H$. The *left derivative* of f in direction $\alpha \in G$ is defined as the map

$$\begin{aligned} d_\alpha^{(l)} f : G &\to H \\ x &\mapsto f(\alpha x) f(x)^{-1}. \end{aligned} \tag{25}$$

Symmetrically, the *right derivative* of f in direction $\alpha \in G$ is the map

$$\begin{aligned} d_\alpha^{(r)} f : G &\to H \\ x &\mapsto f(x)^{-1} f(x\alpha). \end{aligned} \tag{26}$$

The left-translation actions of both G and H are each equivalent to right-translation actions of G and H. Then it is easy to see that each result concerning right-translation action is symmetric to a result on left-translation action. So in this paper, we only focus on the left version and in the remainder we forgot the noun *left*: the derivative of f in direction $\alpha \in G$, will be simply denoted by $d_\alpha f$ and will be the same as $d_\alpha^{(l)} f$.

Definition 11 Let G and H be two finite groups and $f : G \to H$. The map f is said to be *perfect nonlinear* if for each $\alpha \in G^*$, $d_\alpha f$ is balanced *i.e.* for each $(\alpha, \beta) \in G^* \times H$,

$$|\{x \in G | f(\alpha x) f(x)^{-1} = \beta\}| = \frac{|G|}{|H|}. \tag{27}$$

When G and H are Z_2^m and Z_2^n, perfect nonlinearity is a very relevant cryptographic property because it ensures the maximal resistance against the so-called differential cryptanalysis of Biham and Shamir [1]. When $|G| = |H|$, these functions are also known as *planar functions* in finite geometry.

4.2 Bent functions in finite Abelian groups

When considering the case of finite Abelian groups, it is possible to characterize the notion of perfect nonlinearity using the (discrete) Fourier transform; this *dual characterization* leading to an equivalent notion of bent functions. This work has been done recently and independently by Carlet and Ding [2] and Pott [8]. This subsection is then devoted to the presentation of these results.

For the remainder of this subsection, we suppose given a pair (G, H) of finite **Abelian** groups. The main result obtained by the three authors is essentially based on the following lemma.

Lemma 6 *([2]) Let X be a finite nonempty set and $f : X \to H$. The map f is balanced if and only if, for each $\beta \in H^*$, we have*

$$\sum_{x \in X} (\chi_H^\beta \circ f)(x) = 0. \tag{28}$$

In particular, if X is a (finite Abelian) group G, the previous lemma can be re-written as follows: $f : G \to H$ is balanced if and only if for each $\beta \in H^*$, $\widehat{(\chi_H^\beta \circ f)}(e_G) = 0$. This technical result gives a link between balancedness and the Fourier transform which is used to prove the main result given below.

Theorem 1 *([2]) Let $f : G \to H$. The map f is perfect nonlinear if and only if for each $\beta \in H^*$, we have $\forall \alpha \in G$,*

$$|\widehat{(\chi_H^\beta \circ f)}(\alpha)| = \sqrt{|G|}. \tag{29}$$

When G and H are Z_2^m and Z_2^n, a function $f : \mathrm{Z}_2^m \to \mathrm{Z}_2^n$ that satisfies the equalities (29) is called a *boolean bent function*. As perfect nonlinearity, this notion is very important in cryptography because it characterizes the boolean functions that exhibit the best resistance against the linear cryptanalysis of Matsui [4]. By analogy with the boolean case, we will say that a function $f : G \to H$ that satisfies (29) is an *(Abelian) bent function*. The theorem above means that Abelian bentness is strictly equivalent to perfect nonlinearity. In the remainder of this paper, we establish the same kind of dual characterization in the cases where G and/or H can be non Abelian.

5 Bent functions in finite non Abelian groups

5.1 Case where G is non Abelian and H is Abelian

In this subsection, G is a finite **non Abelian** group and H is a finite Abelian group. We first generalize lemma 6 in this context where a non Abelian group occurs.

Lemma 7 *Let $f : G \to H$ and $\rho_0 \in \tilde{G}$ the principal irreducible representation of G. The map f is balanced if and only if for each $\beta \in H^*$,*

$$\widetilde{(\chi_H^\beta \circ f)}(\rho_0) = 0_{End(\mathbb{C})}. \tag{30}$$

Proof First let compute the representation-based Fourier transform of the function $\chi_H^\beta \circ f : G \to \mathrm{C}$ at ρ_0.

$$\begin{aligned}(\widetilde{\chi_H^\beta \circ f})(\rho_0) &= \sum_{x\in G} \chi_H^\beta(f(x))\rho_0(x) \\ &= \sum_{x\in G} \chi_H^\beta(f(x)) Id_{\mathbb{C}} \\ &= \sum_{\gamma\in H} \phi_f(\gamma)\chi_H^\beta(\gamma) Id_{\mathbb{C}} \\ &= \widehat{\phi_f}(\beta) Id_{\mathbb{C}}\end{aligned} \tag{31}$$

where we recall that $\phi_f(\gamma)$ is defined as $|\{x \in G | f(x) = \gamma\}|$.

$\Rightarrow$) Let $\beta \in H^*$ and suppose that f is balanced. Then $\forall \gamma \in H$, $\phi_f(\gamma) = \frac{|G|}{|H|}$ (by definition of balancedness). According to (31), we find $(\widetilde{\chi_H^\beta \circ f})(\rho_0) = \frac{|G|}{|H|} \sum_{\gamma\in H} \chi_H^\beta(\gamma) Id_{\mathbb{C}}$. Since for each $\beta \in H^*$, we have $\sum_{\gamma\in H} \chi_H^\beta(\gamma) = 0$ (by lemma 1), we have $(\widetilde{\chi_H^\beta \circ f})(\rho_0) = 0_{End(\mathbb{C})}$.

$\Leftarrow$) Let suppose that for each $\beta \in H^*$, $(\widetilde{\chi_H^\beta \circ f})(\rho_0) = 0_{End(\mathbb{C})}$. According to (31), we have for each $\beta \in H^*$, $\widehat{\phi_f}(\beta) Id_{\mathbb{C}} = 0_{End(\mathbb{C})}$ and then for each $\beta \in H^*$, $\widehat{\phi_f}(\beta) = 0$. The fourth point of proposition 2 implies then that ϕ_f is constant. Then using the inversion formula, we obtain that for all $\beta \in H$, $\phi_f(\beta) = \frac{1}{|H|}\widehat{\phi_f}(e_H) = \frac{1}{|H|} \sum_{\gamma\in H} \phi_f(\gamma) = \frac{|G|}{|H|}$ (by definition of ϕ_f). Then f is balanced.

□

As in the Abelian case, the previous lemma is fundamental for the dual characterization of perfect nonlinearity. Nevertheless before using it, we need an intermediary result.

Proposition 5 *Let $f : G \to H$ and $\beta \in H$. We define the autocorrelation function of f by*

$$\begin{aligned}AC_{f,\beta} : G &\to \mathrm{C} \\ \alpha &\mapsto ((\widetilde{\chi_H^\beta \circ d_\alpha f})(\rho_0))(1).\end{aligned}$$

Then for all $\rho = \rho_V \in \widetilde{G}$,

$$\widetilde{AC_{f,\beta}}(\rho) = ((\widetilde{\chi_H^\beta \circ f})(\rho)) \circ ((\widetilde{\chi_H^\beta \circ f})(\rho))^*. \tag{32}$$

Proof Let $\rho = \rho_V \in \widetilde{G}$.

$$\begin{aligned}
&\widetilde{AC_{f,\beta}}(\rho) = \sum_{\alpha\in G} AC_{f,\beta}(\alpha)\rho(\alpha)\\
&= \sum_{\alpha\in G} (\widetilde{(\chi_H^\beta \circ d_\alpha f)}(\rho_0))(1)\rho(\alpha)\\
&= \sum_{\alpha\in G}\sum_{x\in G} \chi_H^\beta \circ d_\alpha f(x)\rho_0(x)(1)\rho(\alpha)\\
&= \sum_{\alpha\in G}\sum_{x\in G} \chi_H^\beta(f(\alpha x)f(x)^{-1})\rho(\alpha)\\
&\text{(by definition of } \rho_0)\\
&= \sum_{\alpha\in G}\sum_{x\in G} \chi_H^\beta(f(\alpha x))\overline{\chi_H^\beta(f(x))}\rho(\alpha)\\
&= \sum_{\alpha\in G}\sum_{x\in G} \chi_H^\beta(f(\alpha x))\overline{\chi_H^\beta(f(x))}\rho(\alpha x x^{-1})\\
&= \sum_{\alpha\in G}\sum_{x\in G} \chi_H^\beta(f(\alpha x))\overline{\chi_H^\beta(f(x))}\rho(\alpha x)\circ\rho(x^{-1})\\
&(\rho \text{ is a morphism})\\
&= \sum_{\alpha\in G}\sum_{x\in G} \chi_H^\beta(f(\alpha x))\overline{\chi_H^\beta(f(x))}\rho(\alpha x)\circ\rho(x)^{-1}\\
&= \sum_{\alpha\in G}\sum_{x\in G} \chi_H^\beta(f(\alpha x))\overline{\chi_H^\beta(f(x))}\rho(\alpha x)\circ\rho(x)^{*}\\
&(\rho \text{ is unitary})\\
&= \sum_{x\in G}\left(\sum_{\alpha\in G} \chi_H^\beta(f(\alpha x))\rho(\alpha x)\right)\circ(\overline{\chi_H^\beta(f(x))}\rho(x)^*)\\
&\text{(by linearity)}\\
&= \sum_{x\in G}(\widetilde{(\chi_H^\beta \circ f)}(\rho))\circ(\overline{\chi_H^\beta(f(x))}\rho(x)^*)\\
&= (\widetilde{(\chi_H^\beta \circ f)}(\rho))\circ\left(\sum_{x\in G}\overline{\chi_H^\beta(f(x))}\rho(x)^*\right)\\
&= (\widetilde{(\chi_H^\beta \circ f)}(\rho))\circ(\widetilde{(\chi_H^\beta \circ f)}(\rho))^*.
\end{aligned}$$

□

The dual characterization of perfect nonlinearity in this context is given below. This result generalizes the one of Carlet, Ding and Pott.

Theorem 2 *Let $f : G \to H$. The map f is perfect nonlinear if and only if $\forall \rho = \rho_V \in \widetilde{G}$ and $\forall \beta \in H^*$, we have*

$$(\widetilde{(\chi_H^\beta \circ f)}(\rho))\circ(\widetilde{(\chi_H^\beta \circ f)}(\rho))^* = |G|Id_V. \tag{33}$$

Proof The map f is perfect nonlinear
$\Leftrightarrow \forall \alpha \in G^*,\ d_\alpha f$ is balanced (by definition)
$\Leftrightarrow \forall \alpha \in G^*,\ \forall \beta \in H^*,\ (\widetilde{\chi_H^\beta \circ d_\alpha f})(\rho_0) = 0_{End(\mathbb{C})}$ (according to lemma 7)
$\Leftrightarrow \forall z \in \mathbb{C}, \forall \alpha \in G^*,\ \forall \beta \in H^*,\ (\widetilde{(\chi_H^\beta \circ d_\alpha f)}(\rho_0))(z) = 0$
$\Leftrightarrow \forall z \in \mathbb{C}, \forall \alpha \in G^*,\ \forall \beta \in H^*,\ zAC_{f,\beta}(\alpha) = 0$ (by definition of $AC_{f,\beta}$)

$\Leftrightarrow \forall \alpha \in G^*,\ \forall \beta \in H^*,\ AC_{f,\beta}(\alpha) = 0$
$\Leftrightarrow \forall \rho = \rho_V \in \widetilde{G},\ \forall \beta \in H^*,\ \widetilde{AC_{f,\beta}}(\rho) = AC_{f,\beta}(e_G) Id_V$ (according to the first point of lemma 5).
We have

$$\begin{aligned} AC_{f,\beta}(e_G) &= (\widetilde{(\chi_H^\beta \circ d_{e_G} f)}(\rho_0))(1) \\ &= \sum_{x \in G} \chi_H^\beta(e_H)\rho_0(x)(1) \\ &= \sum_{x \in G} \chi_H^\beta(e_H) \\ &= |G|. \end{aligned} \tag{34}$$

Then f is perfect nonlinear $\Leftrightarrow \forall \beta \in H^*, \forall \rho = \rho_V \in \widetilde{G},\ \widetilde{AC_{f,\beta}}(\rho) = |G| Id_V$
$\Leftrightarrow \forall \beta \in H^*, \forall \rho \in \widetilde{G},\ (\widetilde{(\chi_H^\beta \circ f)}(\rho)) \circ (\widetilde{(\chi_H^\beta \circ f)}(\rho))^* = |G| Id_V$ (according to proposition 5). □

The functions that satisfy formula (33) are the bent functions in this particular context where G is a finite non Abelian group and H is a finite Abelian group.
We can note that this version of bentness is very similar to the one given in theorem 1: the discrete Fourier transform is replaced by its representation-based version, the complex-conjugate is replaced by the adjoint of endomorphisms, the multiplication of complex numbers by the composition of operators and the factor Id_V is added. The discrete Fourier transform of Carlet, Ding and Pott's bent functions is, up to a factor $|G|$, $\mathrm{U}(\mathbb{C})$-valued. Regarding this last notion of bentness, the representation-based Fourier transform, also up to the factor $|G|$, is now $\mathrm{U}(V)$-valued. It is possible to deduce from this theorem a result really similar to the traditional notion of bentness.

Corollary 1 *Let $f : G \to H$. If the map f is perfect nonlinear then we have $\forall \rho = \rho_V \in \widetilde{G}$ and $\forall \beta \in H^*$,*

$$\| \widetilde{(\chi_H^\beta \circ f)}(\rho) \|^2_{End(V)} = |G| \dim_{\mathbb{C}}(V), \tag{35}$$

where $\| \lambda \|^2_{End(V)} = tr(\lambda \circ \lambda^*)$ for $\lambda \in End(V)$.

Proof The result is obvious by using on each member of (33) the trace tr of endomorphisms of V. □

An interesting question, kept open in this paper, is to know if, whether or not, the reciprocal assertion of the previous corollary is true.

5.2 Case where G is Abelian and H is non Abelian

In this subsection, G is a finite Abelian group and H is a finite **non Abelian** group. Another time a technical result similar to both lemmas 6 and 7 is needed to establish a dual characterization of perfect nonlinearity in this context.

Lemma 8 *Let X be a finite nonempty set and $f : X \to H$. Then f is balanced if and only if for each $\rho = \rho_V \in \widetilde{H^*}$, we have*

$$\sum_{x \in X} (\rho \circ f)(x) = 0_{End(V)}. \tag{36}$$

Proof Let $\rho = \rho_V \in \widetilde{H}$. We have

$$\begin{aligned}\sum_{x\in X}(\rho\circ f)(x) &= \sum_{\gamma\in H}|\{x\in X|f(x)=\gamma\}|\rho(\gamma)\\ &= \sum_{\gamma\in H}\phi_f(\gamma)\rho(\gamma)\\ &= \widetilde{\phi_f}(\rho).\end{aligned} \tag{37}$$

$\Rightarrow$) Let suppose that f is balanced and let $\rho \in \widetilde{H}^*$, then we have

$$\sum_{x\in X}(\rho\circ f)(x) = \frac{|X|}{|H|}\sum_{\gamma\in H}\rho(\gamma) = 0_{End(V)}$$

(according to lemma 4).

$\Leftarrow$) Let suppose that for all $\rho = \rho_V \in \widetilde{H}^*$, $\sum_{x\in X}(\rho\circ f)(x) = 0_{End(V)}$. Then the representation-based Fourier transform of $\phi_f : H \to \mathrm{N} \subset \mathrm{C}$ is

$$\rho_V \mapsto \begin{cases} 0_{End(V)} & \text{if } \rho_V \in \widetilde{H}^*,\\ |X| & \text{if } \rho_V = \rho_0.\end{cases} \tag{38}$$

According to lemma 5, we know that ϕ_f is constant and more precisely (according to the proof of the lemma), $\forall\beta \in H$, $\phi_f(\beta) = \frac{1}{|X|}tr(\widetilde{\phi_f}(Id_{\mathbb{C}}))$. But $\widetilde{\phi_f}(Id_{\mathbb{C}}) = \sum_{\gamma\in H}\phi_f(\gamma)Id_{\mathbb{C}} = |X|Id_{\mathbb{C}}$ (by definition of ϕ_f). Then $\forall\beta\in H$, $\phi_f(\beta) = \frac{|X|}{|H|}$ and f is balanced.

□

As in the previous case, we introduce a kind of autocorrelation function and we compute its discrete Fourier transform.

Proposition 6 *Let $f : G \to H$ and $\rho = \rho_V \in \widetilde{H}$. We define the autocorrelation function of f by*

$$\begin{aligned}AC_{f,\rho} : G &\to End(V)\\ \alpha &\mapsto \sum_{x\in G}(\rho\circ d_\alpha f)(x).\end{aligned}$$

Then for all $\alpha \in G$,

$$\widehat{AC_{f,\rho}}^{MD}(\alpha) = (\widehat{(\rho\circ f)}^{MD}(\alpha))\circ(\widehat{(\rho\circ f)}^{MD}(\alpha))^*. \tag{39}$$

Proof Let $\alpha \in G$.

$$\begin{aligned}
&\widehat{AC_{f,\rho}}^{MD}(\alpha) = \sum_{x\in G} \chi_G^\alpha(x) AC_{f,\rho}(x) \\
&= \sum_{x\in G} \chi_G^\alpha(x) \sum_{y\in G} (\rho \circ d_x f)(y) \\
&= \sum_{x\in G} \sum_{y\in G} \chi_G^\alpha(x) \rho(f(xy)) \circ (\rho(f(y)))^* \\
&\text{(since } \rho(x) \text{ is unitary)} \\
&= \sum_{x\in G} \sum_{y\in G} \chi_G^\alpha(xyy^{-1}) \rho(f(xy)) \circ (\rho(f(y)))^* \\
&= \sum_{x\in G} \sum_{y\in G} \chi_G^\alpha(xy) \rho(f(xy)) \circ \overline{\chi_G^\alpha(y)} (\rho(f(y)))^* \\
&= \sum_{y\in G} \widehat{\rho \circ f}^{MD}(\alpha) \circ (\chi_G^\alpha(y) \rho(f(y)))^* \\
&= (\widehat{(\rho \circ f)}^{MD}(\alpha)) \circ (\widehat{(\rho \circ f)}^{MD}(\alpha))^*.
\end{aligned} \tag{40}$$

□

The corresponding notion of bentness in this context is given by the following theorem.

Theorem 3 *Let $f : G \to H$. The map f is perfect nonlinear if and only if $\forall \alpha \in G$, $\forall \rho = \rho_V \in \widetilde{H}^*$,*

$$(\widehat{(\rho \circ f)}^{MD}(\alpha)) \circ (\widehat{(\rho \circ f)}^{MD}(\alpha))^* = |G| Id_V. \tag{41}$$

Proof

$$\begin{aligned}
&\text{f is perfect nonlinear} \Leftrightarrow \forall \alpha \in G^*,\ d_\alpha f \text{ is balanced} \\
&\Leftrightarrow \forall \alpha \in G^*,\ \forall \rho = \rho_V \in \widetilde{H}^*,\ \sum_{x\in G} (\rho \circ d_\alpha f)(x) = 0_{End(V)} \\
&\text{(according to lemma 8)} \\
&\Leftrightarrow \forall \alpha \in G^*,\ \forall \rho \in \widetilde{H}^*,\ AC_{f,\rho}(\alpha) = 0_{End(V)} \\
&\text{(by definition of } AC_{f,\rho}) \\
&\Leftrightarrow \forall \alpha \in G,\ \forall \rho \in \widetilde{H}^*,\ \widehat{AC_{f,\rho}}^{MD}(\alpha) = AC_{f,\rho}(e_G) \\
&\text{(according to proposition 3).}
\end{aligned} \tag{42}$$

But $AC_{f,\rho}(e_G) = \sum_{x\in G} (\rho \circ d_{e_G} f)(x) = \sum_{x\in G} \rho(e_H) = \sum_{x\in G} Id_V = |G| Id_V$. Then according to (40) and (42), f is perfect nonlinear $\Leftrightarrow \forall \alpha \in G,\ \forall \rho = \rho_V \in \widetilde{H}^*$,

$$(\widehat{(\rho \circ f)}^{MD}(\alpha)) \circ (\widehat{(\rho \circ f)}^{MD}(\alpha))^* = |G| Id_V. \tag{43}$$

□

Another time, by using the trace on both sides of (41), we deduce the following corollary. As in the previous case, an interesting question should be to check if this result is or not a sufficient condition for bentness in this particular context.

Corollary 2 *Let $f : G \to H$. If the map f is perfect nonlinear then $\forall \alpha \in G$ and $\forall \rho = \rho_V \in \widetilde{H}^*$,*

$$\| \widehat{(\rho \circ f)}^{MD}(\alpha) \|^2_{End(V)} = |G| \dim_{\mathbb{C}}(V). \tag{44}$$

5.3 Case where G and H are both non Abelian

In this subsection, G and H are both finite **non Abelian** groups.

Let $\rho' = \rho'_W \in \widetilde{H}$ and $B = \{e_i\}_{i=1}^{\dim_{\mathbb{C}}(W)}$ be an orthonormal basis of W (for the scalar product $\langle .,. \rangle_{H,\rho',W}$ of W as introduced by (16)) in which for all $y \in H$, $\rho'(y)$ is a unitary operator. For $(i,j) \in \{1,\dots,\dim_{\mathbb{C}}(W)\}^2$, let define

$$\begin{array}{rcl} \rho'_{ij} : H & \to & \mathbb{C} \\ y & \mapsto & \langle \rho'(e_i), e_j \rangle_{H,\rho',W}. \end{array} \tag{45}$$

In other terms, for each $y \in H$, $\rho'_{ij}(y)$ is simply the coefficient (i,j) of the $\dim_{\mathbb{C}}(W) \times \dim_{\mathbb{C}}(W)$ unitary matrix that represents $\rho'(y)$ in the basis B.
Let see some obvious results on ρ'_{ij} for $(i,j) \in \{1,\dots,\dim_{\mathbb{C}}(W)\}^2$.

1. Let $(y_1,y_2) \in H^2$. We have $\rho'(y_1y_2) = \rho'(y_1) \circ \rho'(y_2)$. Then we have $\rho'_{ij}(y_1y_2) = \sum_{k=1}^{\dim_{\mathbb{C}}(W)} \rho'_{ik}(y_1)\rho'_{kj}(y_2)$;
2. Let $y \in H$. Since $\rho'(y^{-1}) = \rho'(y)^*$ then we deduce that $\rho'_{ij}(y^{-1}) = \overline{\rho'_{ji}(y)}$.

Note also that the identity map Id_W is written in any orthonormal basis of W as the identity matrix and $0_{End(W)}$ is associated, in any basis of W, with the all-zero matrix.

As in the previous subsections, we introduce some kind of autocorrelation function for $f : G \to H$.

Proposition 7 *Let $f : G \to H$, $\rho' = \rho'_W \in \widetilde{H}$ and $(i,j) \in \{1,\dots,\dim_{\mathbb{C}}(W)\}^2$. We define the autocorrelation function of f*

$$\begin{array}{rcl} AC_{f,\rho',i,j} : G & \to & \mathbb{C} \\ \alpha & \mapsto & \sum_{x \in G} (\rho'_{ij} \circ d_\alpha f)(x). \end{array} \tag{46}$$

Then for all $\rho = \rho_V \in \widetilde{G}$,

$$\widetilde{AC_{f,\rho',i,j}}(\rho) = \sum_{k=1}^{dim_{\mathbb{C}}(W)} ((\widetilde{\rho'_{ik} \circ f})(\rho)) \circ ((\widetilde{\rho'_{jk} \circ f})(\rho))^*. \tag{47}$$

Proof Let $\rho = \rho_V \in \widetilde{G}$.

$$\begin{aligned}
&\widetilde{AC_{f,\rho',i,j}}(\rho) = \sum_{x\in G} AC_{f,\rho',i,j}(x)\rho(x)\\
&= \sum_{x\in G}\sum_{y\in G} (\rho'_{ij}\circ d_x f)(y)\rho(x)\\
&= \sum_{x\in G}\sum_{y\in G} \rho'_{ij}(f(xy)f(y)^{-1})\rho(x)\\
&= \sum_{x\in G}\sum_{y\in G}\sum_{k=1}^{\dim_{\mathbb{C}}(W)} \rho'_{ik}(f(xy))\overline{\rho'_{jk}(f(y))}\rho(x)\\
&= \sum_{k=1}^{\dim_{\mathbb{C}}(W)}\sum_{x\in G}\sum_{y\in G} \rho'_{ik}(f(xy))\overline{\rho'_{jk}(f(y))}\rho(xyy^{-1})\\
&= \sum_{k=1}^{\dim_{\mathbb{C}}(W)}\sum_{x\in G}\sum_{y\in G} \rho'_{ik}(f(xy))\overline{\rho'_{jk}(f(y))}\rho(xy)\circ\rho(y)^*\\
&= \sum_{k=1}^{\dim_{\mathbb{C}}(W)}\sum_{x\in G}\sum_{y\in G} \rho'_{ik}(f(xy))\rho(xy)\circ\left(\overline{\rho'_{jk}(f(y))}\rho(y)^*\right)\\
&= \sum_{k=1}^{\dim_{\mathbb{C}}(W)} (\widetilde{(\rho'_{ik}\circ f)}(\rho))\circ\sum_{y\in G}\left(\rho'_{jk}(f(y))\rho(y)\right)^*\\
&= \sum_{k=1}^{\dim_{\mathbb{C}}(W)} (\widetilde{(\rho'_{ik}\circ f)}(\rho))\circ(\widetilde{(\rho'_{jk}\circ f)}(\rho))^*.
\end{aligned} \tag{48}$$

□

Using this autocorrelation function and its Fourier transform we can exhibit the appropriate notion of bentness for this context where both groups G and H are non Abelian.

Theorem 4 *Let $f : G \to H$. The map f is perfect nonlinear if and only if $\forall \rho = \rho_V \in \widetilde{G}$, $\forall \rho' = \rho'_W \in \widetilde{H}^*$, $\forall (i,j) \in \{1,\ldots,\dim_{\mathbb{C}}(W)\}^2$,*

$$\sum_{k=1}^{\dim_{\mathbb{C}}(W)} (\widetilde{(\rho'_{ik}\circ f)}(\rho))\circ(\widetilde{(\rho'_{jk}\circ f)}(\rho))^* = \begin{cases} |G|Id_V & \text{if } i=j,\\ 0_{End(V)} & \text{if } i\neq j.\end{cases} \tag{49}$$

Proof

$$\begin{aligned}
&f \text{ is perfect nonlinear} \Leftrightarrow \forall \alpha\in G^*,\ d_\alpha f \text{ is balanced}\\
&\Leftrightarrow \forall \alpha\in G^*,\ \forall \rho' = \rho'_W \in \widetilde{H}^*,\\
&\qquad \sum_{x\in G}(\rho'\circ d_\alpha f)(x) = 0_{End(W)}\\
&\text{(according to lemma 8)}\\
&\Leftrightarrow \forall \alpha\in G^*,\ \forall \rho'\in\widetilde{H}^*,\ \forall (i,j)\in\{1,\ldots,\dim_{\mathbb{C}}(W)\}^2,\\
&\qquad \sum_{x\in G}(\rho'_{ij}\circ d_\alpha f)(x) = 0\\
&\Leftrightarrow \forall \alpha\in G^*,\ \forall \rho'\in\widetilde{H}^*,\ \forall (i,j)\in\{1,\ldots,\dim_{\mathbb{C}}(W)\}^2,\\
&\qquad AC_{f,\rho',i,j}(\alpha) = 0\\
&\Leftrightarrow \forall \rho_V\in\widetilde{G},\ \forall \rho'\in\widetilde{H}^*,\ \forall (i,j)\in\{1,\ldots,\dim_{\mathbb{C}}(W)\}^2,\\
&\qquad \widetilde{AC_{f,\rho',i,j}}(\rho_V) = AC_{f,\rho',i,j}(e_G)Id_V\\
&\text{(by lemma 5).}
\end{aligned} \tag{50}$$

But $AC_{f,\rho',i,j}(e_G) = \sum_{x\in G}(\rho'_{ij}\circ d_{e_G} f)(x) = \sum_{x\in G}\rho'_{ij}(e_H)$. Since we know that $\rho'(e_H) = Id_W$, then $\rho'(e_H)$ is written in the orthonormal basis B of W as the identity matrix and then $\forall (i,j) \in \{1,\dots,\dim_{\mathbb{C}}(W)\}^2$,

$$\rho'_{ij}(e_H) = \begin{cases} 1 \text{ if } i = j, \\ 0 \text{ if } i \neq j. \end{cases} \tag{51}$$

From this last result, the equality (48) and the equivalence (50), it follows the expected result. □

This case where both groups G and H are non Abelian involves some kind of tensor (or at least of block-matrix) notion of bentness. This is essentially due to the lack of commutativity of both groups.

6 Summary

The different notions of bentness, depending on the fact that the finite groups G and H are Abelian or not, are summarized below.
A function $f : G \to H$ is *bent* (or equivalently perfect nonlinear) if and only if

1. If G and H are Abelian ([2,8]): $\forall(\alpha,\beta) \in G \times H^*$,
$$|\widehat{(\chi_G^{\beta} \circ f)}(\alpha)|^2 = |G|.$$
2. If G is non Abelian and H is Abelian: $\forall(\rho,\beta) \in \tilde{G} \times H^*$ (with $\rho : G \to \mathrm{U}(V)$),
$$(\widetilde{(\chi_H^{\beta} \circ f)}(\rho)) \circ (\widetilde{(\chi_H^{\beta} \circ f)}(\rho))^* = |G| Id_V.$$
3. If G is Abelian and H is non Abelian: $\forall(\alpha,\rho') \in G \times \widetilde{H}^*$ (with $\rho' : H \to \mathrm{U}(W)$):
$$(\widehat{(\rho' \circ f)}^{MD}(\alpha)) \circ (\widehat{(\rho' \circ f)}^{MD}(\alpha))^* = |G| Id_W.$$
4. If G and H are both non Abelian groups: $\forall(\rho,\rho',(i,j)) \in \widetilde{G}\times\widetilde{H}^*\times\{1,\dots,\dim_{\mathbb{C}}(W)\}^2$ (with $\rho : G \to \mathrm{U}(V)$ and $\rho' : H \to \mathrm{U}(W)$),
$$\sum_{k=1}^{\dim_{\mathbb{C}}(W)} (\widetilde{(\rho'_{ik} \circ f)}(\rho)) \circ (\widetilde{(\rho'_{jk} \circ f)}(\rho))^* = \begin{cases} |G| Id_V & \text{if } i = j, \\ 0_{End(V)} & \text{if } i \neq j. \end{cases}$$

References

1. E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems", *Journal of Cryptology*, vol. 4, no. 1, pp. 3-72, 1991
2. C. Carlet and C. Ding, "Highly nonlinear mappings", *Journal of Complexity*, vol. 20, no. 2, pp. 205-244, 2004
3. J. F. Dillon, "Elementary Hadamard difference sets", PhD Thesis, University of Maryland, 1974
4. M. Matsui, "Linear Cryptanalysis Method for DES Cipher", *Advances in Cryptology - Eurocrypt '93*, ser. Lecture Notes in Computer Science, vol. 765, pp. 386-397, 1994
5. K. Nyberg, "Perfect nonlinear S-boxes", *Advances in Cryptology - Eurocrypt'91*, ser. Lecture Notes in Computer Science, vol. 547, pp. 378-386, 1992

6. G. Peyré, "L'algèbre discrète de la transformée de Fourier", *Collection Mathématiques à l'Université*, Ellipses, 2004
7. L. Poinsot, "Multidimensional bent functions", to appear in *GESTS International Transactions in Computer Science and Engineering*, vol. 18, no. 1, pp. 185-195, 2005
8. A. Pott, "Nonlinear functions in Abelian groups and relative difference sets", *Discrete Applied Mathematics*, vol. 138, issue 1-2, pp. 177-193, 2004
9. O. S. Rothaus, "On bent functions", *Journal of Combinatorial Theory A*, vol. 20, pp. 300-365, 1976